ANALOG DEVICES

産業用サイバーセキュリティの詳細

VISIT ANALOG.COM/CYBERSECURITY

最新デジタル・ファクトリの信頼できるエッジ

デジタル・トランスフォーメーションは産業界の変化を促進する役割を果たしてきましたが、その一方で、オートメーション促進とプロセス効率向上のためのリアルタイムの意思決定を可能にするために、デジタル化によって生成されるデータは増え続けています。このデータを最大限に活用するため、デジタル企業のネットワーク化がますます進んでいますが、これを実現するには、OT（運用および制御技術）ネットワークとオフィスのIT（情報技術）ネットワークを融合させる必要があります。この急速な技術の進歩によってインテリジェント・エッジの力が大きく向上し、エッジとクラウドをシームレスに接続して運用することが可能になりました。デジタル・コネクティビティ技術の採用が拡大して帯域幅が増大し、実際のプロセス・プラントや工場のあらゆる側面から集められた情報へのアクセスも増えるのに伴い、サイバーセキュリティ上の脆弱性レベルの増大についても検討する必要が生じています。新たな産業用イーサネット技術インフラストラクチャによってすべてのノードでIPアドレスの指定が可能になり、ゲートウェイ・デバイスも使われなくなったことで、サイバー攻撃からデバイスとシステムのセキュリティを確保することが極めて重要になっています。これらの攻撃は、その潜在的なコストが極めて高くなっているだけでなく、安全に関係する制御システムにおいては、人間の生命を危険にさらすおそれすらあります。

現在、産業用自動制御システム（IACS）がサイバー攻撃に対するレジリエンスを備えるようになった世界で、多くの企業が業務の進め方について考える必要に迫られています。制御システムがコマンドを管理して他のデバイスの動作を調整しますが、攻撃を受けた場合は製造インフラストラクチャ全体に脅威が及びます。サイバー攻撃には侵襲的な攻撃と非侵襲的な攻撃があります。侵襲的な攻撃の場合、サイバー犯罪者はデバイスのエンクロージャを開いて、メモリ内容の操作、ファームウェアの置き換え、あるいはPCB配線パターンのプロービングなどを行います。非侵襲的な攻撃は通常、通信ポートやデバイスのファームウェアに隠れたセキュリティ上の不備を通じて、リモートで行われます。

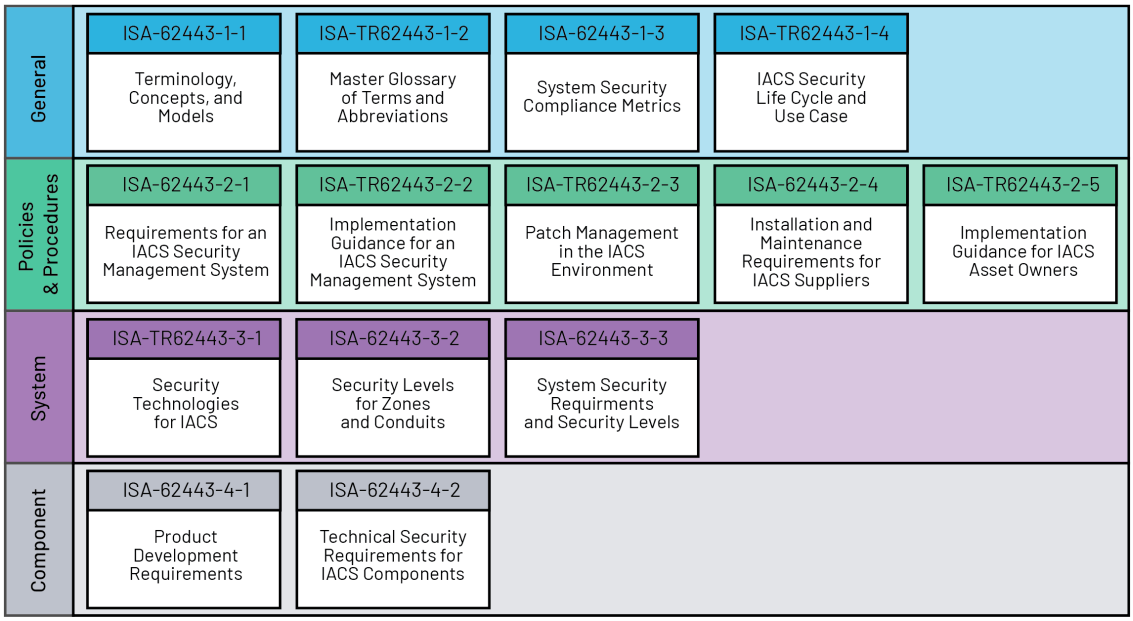


図1：
IEC 62443シリーズのセキュリティ規格

EUのサイバー・レジリエンス法（CRA）は、EU内で販売されるデジタル製品のサイバーセキュリティについて規定するEUの新しい法律で、EU市場向けに設計された「デジタル要素を含む製品（Products with Digital Elements: PDE）」を扱う世界中のメーカー、デベロッパー、およびベンダーに影響を与えます。この法律は、製品CEマークの表示義務導入を含めて、2027年までに施行される予定です。これにより、新製品の開発サイクルにセキュリティに関する検討を前もって組み込むことを優先させなければならなくなりました。さもないと、現在開発中の新製品が、2027年以降にEU市場で販売する製品に求められる基準を満たさなくなってしまうおそれがあるからです。

詳細については、アナログ・デバイセズの技術記事「IEC 62443シリーズの規格：サイバー攻撃からインフラストラクチャを保護する方法」をご覧ください。

CRAの規定の採用を促進するため、欧州ネットワーク情報セキュリティ機関（ENISA）は、EU CRAの要求事項とIEC 62443-4規格の対応付けを行いました。
IEC 62443シリーズの規格は、オートメーション・プロセスや制御プロセスにおける運用および制御技術に関するサイバーセキュリティの問題に対処するために考えられたものです。この最新の規格は、攻撃を防止してその影響を軽減するために、幅広い層のセキュリティを提供します。規格の内容は4つのレベルとカテゴリに分類されています。すなわち、シリーズ全体に共通する「概要」、IACSセキュリティに関わる方法とプロセスに焦点を当てた「ポリシーと手順」、システム・レベルの要求事項の概略を示した「システム」、およびIACS製品の詳細な要求事項を定めた「コンポーネント」です。

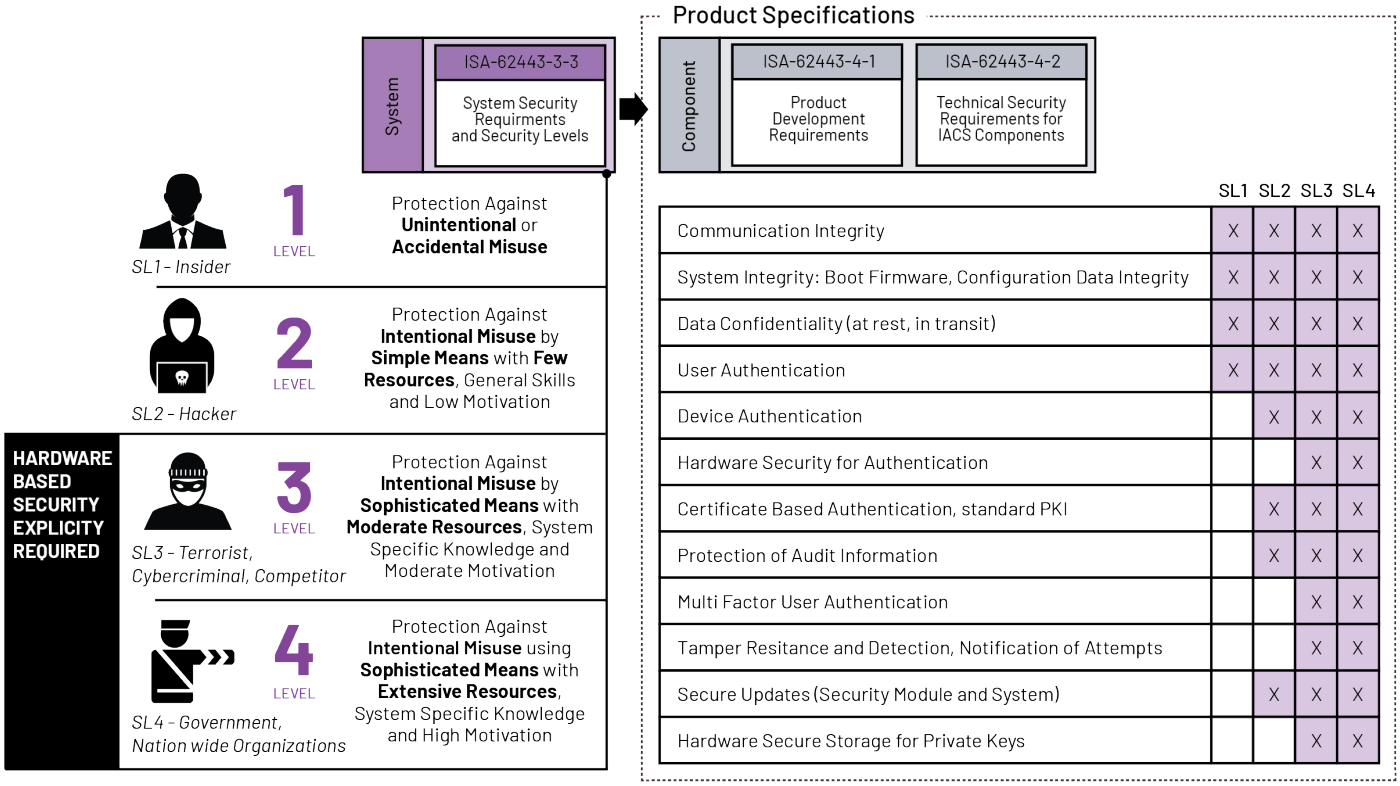


図2：
IEC 62443のコンポーネント要求と必要とされるシステム・セキュリティ・レベルの対応

安全なコンポーネントを設計するには、まずリスク・アセスメントを行い、デバイスが必要とするセキュリティのレベルを決定することが重要です。このアセスメントの結果によって、デバイスが耐えなければならないセキュリティ・レベルが明らかになります。つまり、通常は意図せぬ不正使用や過失による不正使用であるレベル1の「インサイダー」攻撃、限定的なリソースで意図的に損害を与えようとするレベル2の「ハッカー」、そしてシステムに損害を与えるという意図と高度なリソースの下に攻撃を行うレベル3の「サイバー犯罪」とレベル4の「政府」の関与です。

ISA-62443-3-3「システム・セキュリティ要求とセキュリティ・レベル」とコンポーネント・レベル仕様（ISA-62443-4-1、ISA-62443-4-2）の組合せで、サイバー攻撃に耐え得る安全なコンポーネントの設計方法を規定しています。求められるセキュリティ・レベルに基づいて、設計の中に具体的な要求事項を組み込む必要があります。すべてのレベルにおいて、取り扱いに注意を要するとされるデータを秘匿できる必要があります。セキュリティ・レベルSL2～SL4にはデバイス認証が必要で、SL3～SL4での運用の実現を目指すデバイスについてはプライベート鍵のハードウェア・セキュア・ストレージが仕様規定されています。アナログ・デバイセズのセキュア製品開発ライフサイクルは、IEC-62441-4-1:2018の認証を受けています。

産業分野のセキュリティにおける脆弱性の理解

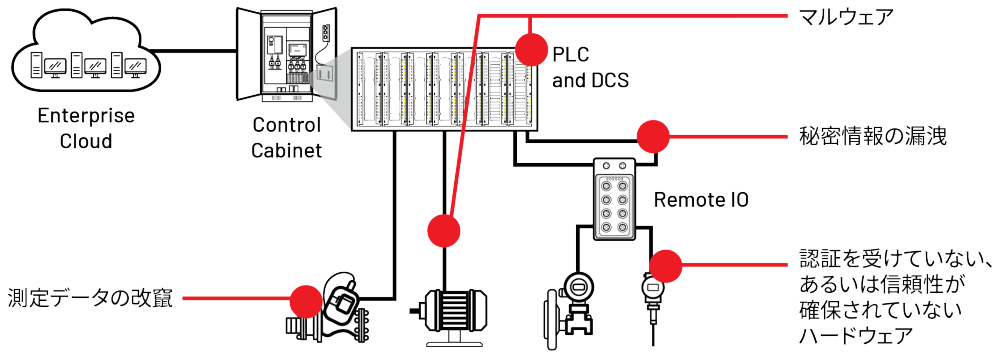


図3:
産業アプリケーションにおける一般的なセキュリティ脆弱性

産業環境の中には、運用するインフラストラクチャの完全性を確保するために、セキュリティを確保する必要のある脆弱な領域がいくつかあります。ここで、その4つの一般的な領域を考えてみます。いずれもターンキー・セキュアICを使ってセキュリティを確保することができますが、これはセキュア鍵ストレージなどの必須メカニズムを組み込むことによって行うため、IACSコンポーネント・デベロッパーが複雑なセキュリティ・プリミティブ設計にリソースを費やさなくても済むようにします。セキュリティが確保されていないシステムに**セキュアIC**を追加すれば、アーキテクチャを設計し直さなくてもシステム・セキュリティのレベルを上げることができます。それには、強力な暗号化機能を組み込んだ特殊なデバイスが必要ですが、一方で、様々なシステムレベルのセキュリティ機能をサポートできる十分な柔軟性を備えている必要もあります。具体的な推奨製品については、選択表を参照してください。

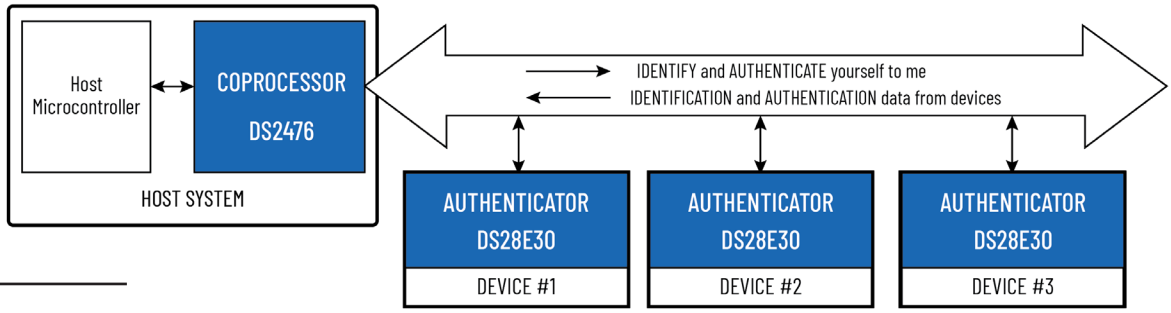


図4:
暗号化を容易にするセキュア認証用ICとセキュア・コプロセッサ

認証を受けていない、あるいは信頼性が確保されていないハードウェア

デバイス間での信頼性の確立は、チャレンジ／レスポンス**認証**を使って実現できます。この認証方法は、対称認証の場合は共有秘密鍵に依存し、非対称認証の場合はプライベート／公開鍵ペアに依存します。公開鍵は公開用に設計されていますが、秘密鍵とプライベート鍵は共にセキュリティ・リスクを伴い、盗まれた場合はネットワーク全体がリスクに曝されます。

公開鍵は秘密にしておく必要はありませんが、その公開鍵が本物であるかどうかを知ることが重要です。デバイスは、デジタル証明書を発行する第三者機関である認証局（CA）によって証明された公開鍵とデバイスIDを持つことができます。鍵認証プロセスにおいては、CAの公開鍵を使って、提供されたデバイスの公開鍵が本物であることを確認できます。

チャレンジ／レスポンス認証は、ノンスと呼ばれる真のランダム・ビット・ストリームを生成する能力に依存しています。データの交換ごとに高いランダム性で生成されるノンスは、「リプレイ攻撃」の可能性からシステムを保護します。セキュア認証用ICは、チャレンジ／レスポンス認証を行うことのできるターンキー認証ソリューションとして使用できます。

秘密情報の漏洩

デバイス内の保存データ、あるいはネットワーク上の他のシステムとの通信時に転送されるデータの保護は暗号化に依存しています。秘密情報の漏洩は、高度暗号化規格（AES）などの実績ある**暗号化**方式を使って防ぐことができます。

攻撃がデバイス・レベルで行われ、データがデバイス内に保存されている状況では、たとえメモリにアクセスされたとしても、セキュア・メモリ・ストレージにより、データはすべて製造時に個々のデバイスのランダム性を利用して物理複製困難関数（PUF）を生成する方法を使用して暗号化されています。PUFをベースとするアナログ・デバイセズのChipDNA®**セキュア認証用IC**は、各鍵をICの精密なアナログ特性として生成し、メモリには保存しません。そのため、既知のすべての侵襲的攻撃ツールや攻撃方法に対して高い耐性を備えています。

データの転送時には、メッセージ・データを暗号化すれば、ネットワーク上の通信を傍受している者に秘密情報が漏洩するのを防ぐことができます。トランスポート層セキュリティ（TLS）プロトコルは、転送データの保護に最も広く使われているプロトコルで、通信の**真正性**、**完全性**、および**機密性**を確保することができます。

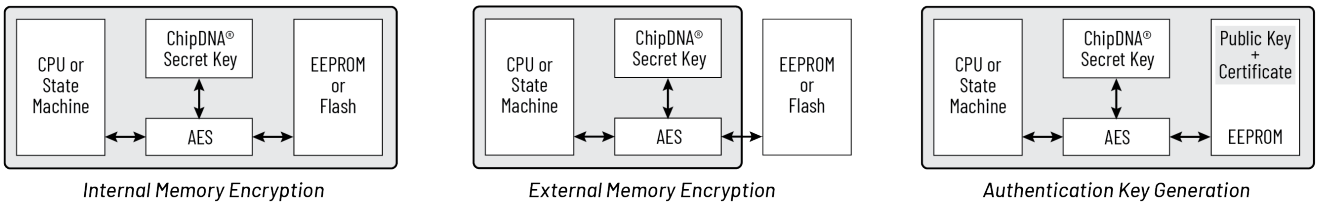


図5：
ChipDNA®によるPUFセキュリティの構成

マルウェア

インターネットのようなセキュリティが確保されていないネットワークに接続されたデバイスは、マルウェアによる攻撃に対して脆弱になり得ます。メーカーによるアップデートが必要なデバイスには、そのアップデートが正式で改竄されていないことを確認するための手段が必要です。**電子署名**を使用すれば、検証されたファームウェアのみを受け入れることができます。セキュア・ブート機能を備えたデバイスは、パワーアップ時にデバイスのファームウェア認証を行います。改竄されたファームウェアがデバイスに入り込んだ場合、そのファームウェアの暗号はメーカーが最初にデバイスに実装したものと一致しなくなり、電子署名が無効となるため、システムがブート・アップを拒否します。

測定データの改竄

データの操作、つまりエッジ・デバイスの測定データ改竄が行われると、システムの健全性を正しく認識できなくなるおそれがあります。より多くのシステムが自動化されるのに伴い、データに基づく意思決定は、信頼できる測定データから行うことができるようにすることが不可欠です。悪意を持った者がエッジ・デバイスの動作に影響を与えようとしたり、ステータス・メッセージに手を加えようとしたりした場合は、署名を通じてコマンドを検証すれば、改竄された測定データが業務に悪影響を与える可能性を排除することができます。

重要な点

システムのセキュリティを確保するには、**認証**機能を使って信頼できる接続を確立する能力がデバイスに求められます。悪意ある者が産業用プロセスを制御するために悪用する可能性のある潜在的な攻撃ポイントを最小限に抑えるため、デバイスには暗号化と復号化を使って情報の**機密性**を確保する能力と、コマンドの**完全性**を検証できる能力が求められます。アナログ・デバイセズのターンキー・セキュアICはこれらの能力を提供し、IACSのアーキテクチャを設計し直すことなく、システムのセキュリティを強化します。

デジタル証明書とプロビジョニング

送信者の**デジタル署名**によって署名されたメッセージは、メッセージがその送信者から送信され、内容が改竄されいていないことを証明するために使用できます。しかし、デジタル署名だけで送信者の身元を証明することはできません。身元の証明は**デジタル証明書**を使って行われます。このデジタル書類には公開鍵と、その鍵の所有者を確認するために使われるID情報が含まれています。アナログ・デバイセズがサービスとして、お客様に代わり、証明書と鍵をプログラムすることができます。デジタル証明書と安全なプロビジョニング・サービスを利用することにより、各種の産業組織はサイバーセキュリティ・インフラストラクチャを大幅に強化し、組織の重要なシステムとデータの完全性、機密性、そして真正性を確保することができます。

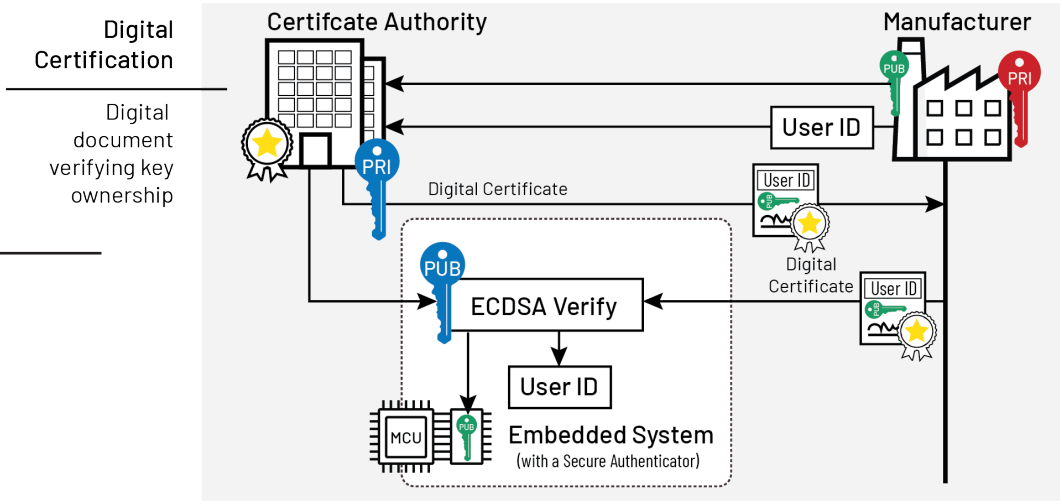


図6:
認証局を使ってデジタル証明書を作成

ファームウェア・アップデート

重要なファームウェアのアップデートは、署名されたメッセージを使い、そのファームウェアが認証済みで変更されていないことも保証した上で、フィールド・デバイスに展開することができます。

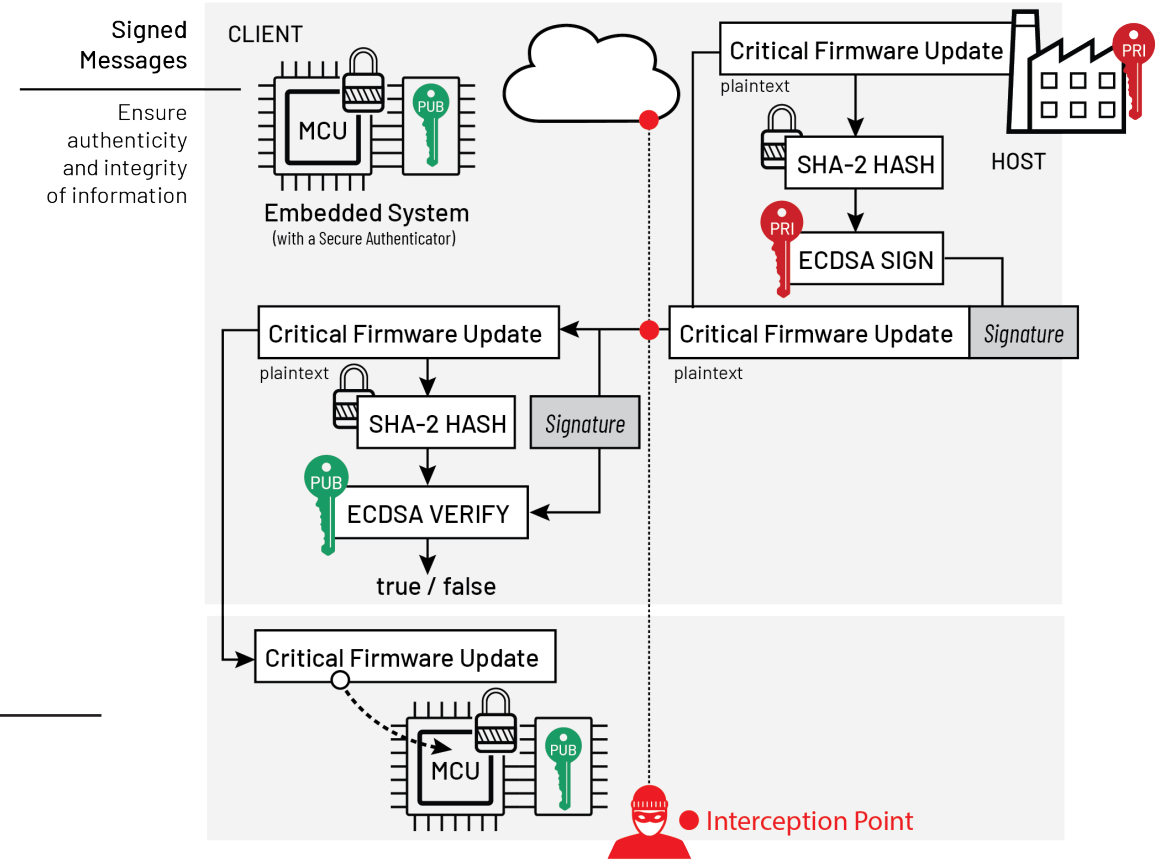
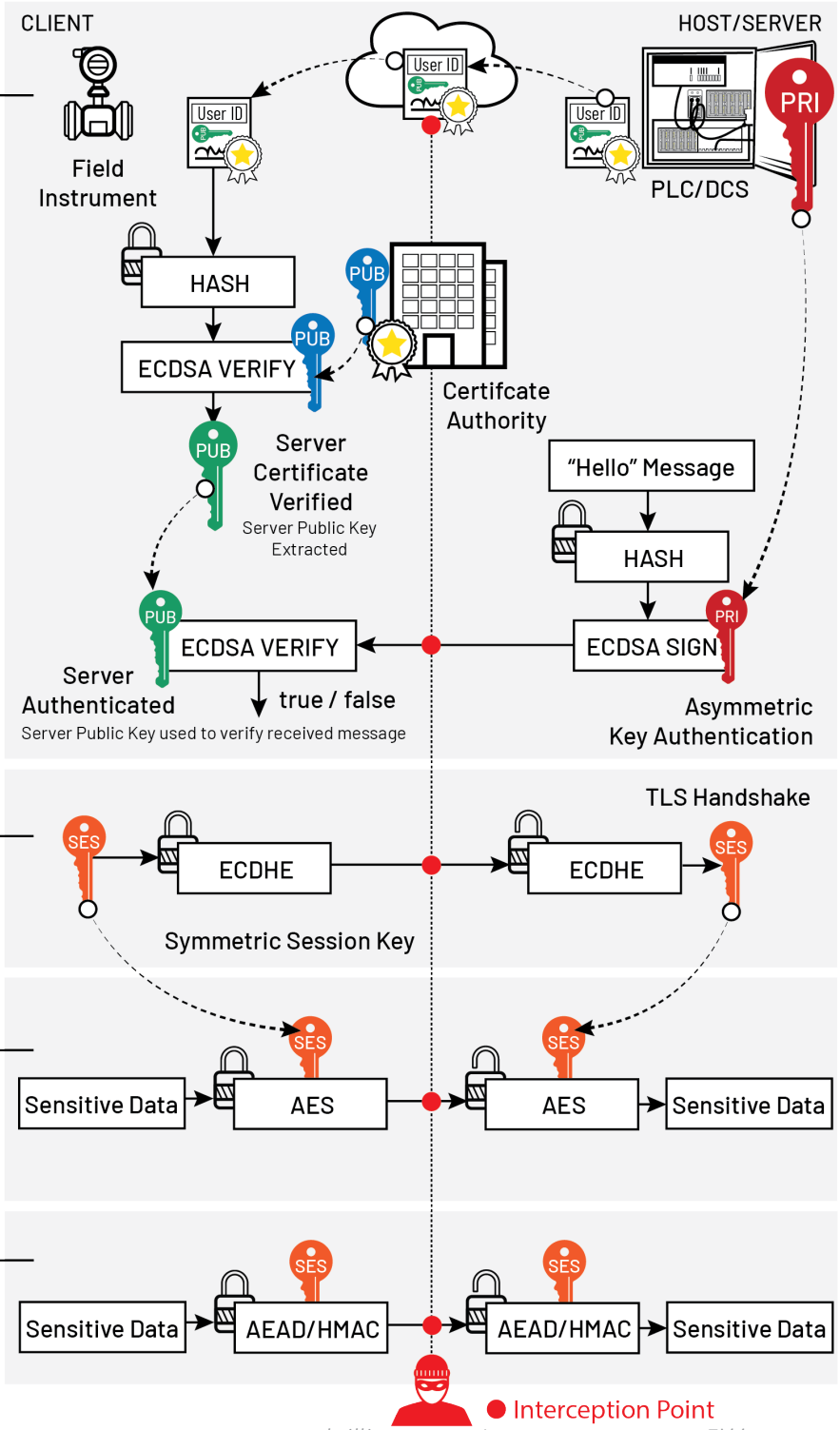


図7:
ファームウェア・アップデート・プロセス

ハードウェア認証とセキュア通信

ハードウェア認証プロセスは、ホスト（PLC）とクライアント（フィールド計測器）間での鍵ペアの交換から開始されます。以下に、2段階で行われる証明書ベースの認証プロセスを示します。第1段階では、ホストの公開鍵が信頼できるものであることを確認するために、クライアントがCA公開鍵を使ってホスト／サーバーの証明書を検証します。次に、公開鍵を使用して、ホストによって計算されたノンス（この場合はその前に交換された「Hello」データ）の署名を検証します。TLSプロトコルでは、サーバーが認証されると、ECDHまたはECDHEの対称アルゴリズムを使って共有通信鍵（セッション鍵）が作られます。更にこのセッション鍵は、サーバーとクライアントが秘密情報を交換できるようにペイロード・データの暗号化に使われます。TLSは、認証された暗号化（AES GCMやAES CCMなど）を使用するか、HMAC（Hash-based Message Authentication Code：ハッシュベースのメッセージ認証コード）を付加することによって完全性を保証します。通信終了後、セッション鍵は破棄されます。

図8：
ハードウェア認証と通信プロセス



一般的に使われるサイバーセキュリティ用語については、こちらの用語集を参照してください。

ADI Assure™は、永続的な保証状態を実現するために、セキュリティ上の脅威に対して確実な保護を提供する一連の製品で構成されています。アナログ・デバイセズの信頼できるエッジ・ソリューションは、セキュリティ境界をデータ発生点の近くまで拡大するので、その真正性と信憑性に関わる信頼度を高めることができます。アナログ・デバイセズは、顧客が産業分野のサイバーセキュリティ標準と法的要求を迅速に満たし、その製品の寿命期間全般にわたるセキュリティ上の脅威増大に対する防御強化の支援に取り組んでいます。 **ChipDNA® PUF**、耐タンパ性を備えた鍵の保管、および高度な暗号化アルゴリズムといったアナログ・デバイセズの最先端技術は、セキュリティ・アーキテクチャを強化して、侵襲的および非侵襲的攻撃に対する抵抗力を強化します。ハードウェアベースのRoT（Root of Trust）とソフトウェア・サービスによるスケーラブルで柔軟なセキュリティ・ソリューションで構成されるアナログ・デバイセズの豊富なポートフォリオは、長期間にわたる保護を提供します。更に、組込みも容易で、最終的にはシステムを安全に保護し、サイバーセキュリティの認証プロセスを加速して、長期的なレジリエンスを実現します。

ハードウェア認証、偽造防止、キャリブレーション、および利用管理用デバイスの選択

AUTHENTICATORS	Secret Key SHA-2	Secret Key SHA-3	Public Key ECDSA	Secret Key SHA-2 & Public Key ECDSA
I2C	DS28C22	DS28C50* DS28C16	DS28C36* DS28C39*	DS28C40
1-Wire	DS28E(L)25 DS28E(L)22 DS28E(L)15	DS28E50* DS28E16	DS28E38* DS28E39* DS28E30	DS28E36 DS28E40
NFC	MAX66240 MAX66242	MAX66250		
COPROCESSORS				
I2C	DS2465	DS2477*		DS2476 DS2478
NFC	MAX66300	MAX66301		

** ChipDNA® PUF Technology*

セキュア・ブート、セキュア・ファームウェア・アップデート、セキュア通信、およびTLSサポート用のセキュアIC

SECURE ELEMENT		ECDSA	ECDH	AES 128/256	Certificates	TLS Software Stack
SPI	DS28S60*	X	X	X	Custom	
	MAXQ1065*	X	X	X	x.509	OpenSSL, mbedTLS, WolfSSL

** ChipDNA® PUF Technology*

ANALOG DEVICES

VISIT ANALOG.COM/CYBERSECURITY